SRI VENKATESWARA COLLEGE OF ENGINEERING,

(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)

M.Tech CYBER FORENSICS AND INFORMATION SECURITY

CURRICULUM AND SYLLABUS

REGULATION – 2022

CHOICE BASED CREDIT SYSTEM

Curriculum Revision No:	00	Board of Studies recommendation date :	16.09.2022	Academic Council Approved date:	
Salient Points of the revision	01.	Decided to keep the same R2018 curriculum and syllabus as it is framed in the year 2021			
	02.				
	03.				
	04.				
	05.				

Note: Times new Roman font and size 12 should be used throughout the document if specific size is not mentioned.

SRI VENKATESWARA COLLEGE OF ENGINEERING,

(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)

REGULATIONS2022

M.Tech CYBERFORENSICS AND INFORMATION SECURITY

CHOICEBASEDCREDITSYSTEM

PROGRAM EDUCATIONAL OBJECTIVES(PEOs)

I. Evolve as globally competent cyber security professionals, researchers and entrepreneurs possessing 21st century skills, to define the architecture, design, and management of the security of an organization

II. Possess in-depth knowledge and skill sets in Cyber Security to monitor, prepare, predict, detect respond and prevent cyber-attacks and ensure enterprise security.

PROGRAM OUTCOMES(POs)

PO GRADUATEATTRIBUTES

1. An ability to independently carry out research /investigation and development work to solve practical problems.

2. An ability to write and present a substantial technical report/document.

3. Students should be able to demonstrate a degree of mastery over the area as per the specialization of the program. The mastery should be at a level higher than the requirements in the appropriate bachelor program

PEO's–PO's&PSO'sMAPPING: (Example)

POs	PEOs	
	I	II
1.	✓	✓
2.	✓	✓
3.	✓	✓

SRI VENKATESWARA COLLEGE OF ENGINEERING,

(An Autonomous Institution, Affiliated to Anna University, Chennai – 600025)

REGULATIONS2022

CHOICEBASEDCREDITSYSTEM

M.Tech CYBERFORENSICS AND INFORMATION SECURITY

CURRICULUM

SEMESTERI

Sl. No.	Course Code	CourseTitle	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	MA22182	Mathematical Foundations For Information Security	FC	3	1	0	4	4		F
2	CF22101	Foundations of Cyber Security	PC	3	1	0	4	4	-	F
3	CF22102	Advanced Operating Systems	PC	3	0	0	3	3	-	F
4	CF22103	Network Principles And Security	PC	3	0	0	3	3	-	F
5	CF22104	Computer Forensics And Digital Evidence	PC	3	0	0	3	3	-	F
6	GR22251	Introduction to Research Methodology & IPR (Common to all branches)	MC	3	0	0	3	3	-	F
Practical Subjects										
7	CF22111	Network Design and Security Laboratory	PC	0	0	3	2	3	-	F
8	CF22112	Ethical Hacking Essentials Laboratory	PC	0	0	3	2	3	-	F
Total				18	2	6	24	26		

SEMESTER II

Sl. No.	Course Code	CourseTitle	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	CF22201	Fundamentals to Security in Biometrics	PC	3	0	0	3	3	-	M
2	CF22202	Digital Forensics and Digital Investigations	PC	3	1	0	4	4	-	M
3	CF22203	Blockchain for Security	PC	3	0	0	3	3	-	F
4	CF22204	Internet of Things And Security	PC	3	1	0	4	4	-	F
5		Professional Elective I	PE	3	0	0	3	3	-	F
Practical Subjects										
6	CF22211	IoT and Blockchain Laboratory	PC	0	0	3	2	3	-	F
7	CF22212	Digital Forensics Laboratory	PC	0	0	3	2	3	-	F
8	CF22213	CaseStudy I – Forensic Investigations	EEC	0	0	2	1	2	-	F
Total				15	2	8	22	25		

Semester III

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	****	Professional Elective - II	PE	3	0	0	3	3	-	M
2	****	Professional Elective - III	PE	3	0	0	3	3	-	M
3	****	Professional Elective - IV	PE	3	0	0	3	3	-	M
Practical Subjects										
4	CF22311	Project Work Phase - I	EEC	0	0	12	6	12	-	F
Total				9	0	12	15	21		

Semester IV

Sl. No.	Course Code	Course Title	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	CF22411	Project Work Phase - II	EEC	0	0	24	12	24	-	F

Total Credit : 73

PROFESSIONAL ELECTIVE

Sl. No.	Course Code	CourseTitle	Category	Periods Per Week				TOTAL HOURS	Pre-requisite	Position
				L	T	P	C			
1	CF22002	Penetration and Application Testing	PE	3	0	0	3	3	-	M
2	CF22004	Applied Cryptography	PE	3	0	0	3	3	-	M
3	CF22006	Data Mining Techniques	PE	3	0	0	3	3	-	M
4	CF22008	Network Virtualisation	PE	3	0	0	3	3	-	M
5	CF22010	Cloud Computing Technologies	PE	3	0	0	3	3	-	M
6	CF22001	Energy Aware Computing	PE	3	0	0	3	3	-	M
7	CF22003	Advanced Infrastructure Management	PE	3	0	0	3	3	-	M
8	CF22005	Machine Learning Techniques	PE	3	0	0	3	3	-	M
9	CF22007	Intrusion Detection and Prevention Systems	PE	3	0	0	3	3	-	M
10	CP22008	Social Network Analysis	PE	3	0	0	3	3	-	M
11	CF22011	Principles of Secure Coding	PE	3	0	0	3	3	-	M
12	CF22013	Trust Management in E – Commerce	PE	3	0	0	3	3	-	M
13	CF22015	Biometric Image Processing	PE	3	0	0	3	3	-	M
14	CF22017	Cyber Security Management and Cyber Laws	PE	3	0	0	3	3	-	M
15	CF22019	Malware Analysis and Reverse Engineering	PE	3	0	0	3	3	-	M
16	CF22021	Data Analytics and Business Intelligence	PE	3	0	0	3	3	-	M
17	CF22023	Wireless Security	PE	3	0	0	3	3	-	M

MA22182 MATHEMATICAL FOUNDATIONS FOR INFORMATION SECURITY

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

1. To understand the concepts of number theory which play an important role in computer science and cryptography.
2. To understand basic concepts of various algebraic structures used in computer science.
3. To understand the concepts of advanced algebraic structures used in computerscience
4. To understand the basic mathematical principles and functions that form the foundation for coding theory
5. To understand basics of elliptic curves and pseudo random numbers and its usage

UNIT I NUMBERTHEORY 12

Introduction - Divisibility - Greatest common divisor - Prime numbers - Fundamental theorem ofarithmetic - Fermat numbers - Euclidean algorithm - Fermat’s theorem - Euler totient function -Euler’s theorem. Congruences - Definition - Basic properties of congruences - Residue classes -Chinese remainder theorem.

UNIT II ALGEBRAICSTRUCTURES I 12

Groups – Cyclic groups, Cosets, Modulo groups - Primitive roots - Rings – Sub rings, ideals and quotient rings.

UNIT III ALGEBRAICSTRUCTURES II 12

Integral domains, Fields–Finite fields - Classification - Structure of finite fields.

UNIT IV CODINGTHEORY 12

Introduction - Basic concepts - Codes, minimum distance, equivalence of codes, Linear codes-Generator matrices and parity - Check matrices - Hamming codes.

UNIT V ELLIPTICCURVESANDPSEUDORANDOMNUMBERGENERATION 12

Discrete Logarithm - Elliptic curves - Introduction to Pseudo random numbers.

TOTAL: 60 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Grasp the concepts of number theory and their applications to cryptography.
CO2	Prove statements and construct examples of some classes of groups and rings.
CO3	Explain integral domain field and finite field and perform an in-depth analysis of various algebraic structures used in computer science.
CO4	Identify the mathematical principles and functions and apply them to the concept of coding theory
CO5	Gain knowledge on discrete logarithms, elliptic curves and pseudo random numbers.

TEXT BOOKS:

1. KennethHRossen,DiscreteMathematicsanditsApplications,SeventhEdition,McGraw Hill,2012.
2. RudolfLidl,GunterPilz,AppliedAbstractAlgebra,SecondEdition,Springer,1998.
3. D.S.Malik,J.Mordeson,M.K.Sen,Fundamentalsofabstractalgebra,McGrawHill,1 997.
4. JosephA.Gallian,ContemporaryAbstractAlgebra,Narosa,1998.
5. L.Washington,EllipticCurves:NumberTheoryandCryptography,Chapman&Hall CRC,2003.

REFERENCES:

1. Niven,H.S.Zuckerman,H.L.Montgomery,Anintroductiontothetheoryofnumbers,Jo hnWiley andSons,2001.
2. FraleighJ.B.,Afirstcourseinabstractalgebra,PearsonEducation,2005.
3. DouglasRStinson,Cryptography:TheoryandPractice,CRCPress,2015**.**

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**1**		**3**
2.	**1**		**3**
3.	**1**		**3**
4.	**1**		**3**
5.	**1**		**3**

CF22101 FOUNDATIONS OF CYBERSECURITY

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

1. Understand various block cipher and stream cipher models
2. Describe the principles of public key cryptosystems, hash functions and digital signature
3. To get a firm knowledge on CyberSecurity Essentials

UNIT I INTRODUCTIONTOSECURITY 12

Data Encryption Standard-Block cipher principles-block cipher modes of operation-Advanced Encryption Standard (AES) - TripleDES - Blowfish - RC5algorithm

UNIT II PUBLICKEYCRYPTOGRAPHYANDHASHALGORITHMS 12

Principles of public key cryptosystems-The RSA algorithm-Key management - Diffie Hellman Key exchange -Hash functions - Hash Algorithms (MD5, Secure Hash Algorithm)

UNIT III FUNDAMENTALSOFCYBERSECURITY 12

How Hackers Cover Their Tracks - Fraud Techniques - Threat Infrastructure-Techniques to Gain a Foothold (Shellcode, SQL Injection, Malicious PDF Files)- Misdirection, Reconnaissance, and Disruption Methods

UNIT IV PLANNING FOR CYBERSECURITY 12

Privacy Concepts -Privacy Principles and Policies -Authentication and Privacy - Data Mining -Privacy on theWeb-Email Security-Privacy Impacts of Emerging Technologies

UNIT V CYBERSECURITYMANAGEMENT 12

Security Planning - Business Continuity Planning - Handling Incidents - Risk Analysis - DealingwithDisaster–LegalIssues–ProtectingprogramsandData–Informationandthelaw–RightsofEmployeesandEmployers-EmergingTechnologies-TheInternetofThings-CyberWarfare

TOTAL: 60 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Implement basic security algorithms required by any computing system
CO2	Analyze the vulnerabilities in any computing system and hence be able to design a security solution
CO3	Analyze the possible security attack in complex real time systems and their effective counte rmeasures
CO4	Enumerate various governing bodies of cyberlaws
CO5	Impart various privacy policies for an organization

REFERENCES:

1. WilliamStallings,“Cryptography and Network Security”,Pearson Education, 6th Edition,2013.
2. CharlesP.PfleegerShariLawrencePfleegerJonathanMargulies,SecurityinComputing,5th Edition,PearsonEducation,2015.
3. Graham,J.Howard,R.,Olson,R.,CyberSecurityEssentials,CRCPress,2011.
4. GeorgeK.Kostopoulous,CyberSpaceandCyberSecurity,CRCPress,2013.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**3**	**1**	**3**
2.	**3**	**1**	**3**
3.	**3**	**1**	**3**
4.	**3**	**1**	**3**
5.	**3**	**1**	**3**

CF22102 ADVANCED OPERATIN GSYSTEMS

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

1. Have a detailed knowledge on Operating system concepts
2. Understand the need for operating system security
3. Administer an open source Operating System

UNIT I OPERATINGSYSTEMS : OVERVIEW 9

Operating System structure and operations - Process Management -Memory Management–Storage Management - Protection and Security – Process Scheduling–Interprocess communication - Multi threading models- Semaphores – Monitors - Deadlocks- Mutexes- Critical Section problem

UNIT II MEMORY MANAGEMENT IN OPERATINGSYSTEM 9

Swapping–Contiguous Memory Allocation– Segmentation – Paging –VirtualMemory: Demand Paging – Page Replacement – Allocation of Frames – Thrashing – Allocating KernelMemories

UNIT III LINUX SYSTEM ADMINISTRATION 9

Requirements for a Linux Administrator – Server Requirements–Logging in Remotely–Network configuration – Providing DNS – Adding Relational DB – Configuring mail securely –Adding FTP services–Synchronizing the system clock–Installing perl modules

UNIT IV OPERATING SYSTEMS : TRUST MODEL 9

Security Goals – Trust and Threat Model – Protection System – Reference Monitor – Secure Operating System–Assessment Criteria – Mutics History–Multics System and Security

UNIT V OPERATINGSYSTEMSSECURITY 9

System History – Unix and Windows History – Unix Security – Windows Security – Verifiable Security Goals – Security Kernels – Securing Commercial Operating Systems

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Enumerate the basic functionalities of operating system
CO2	Demonstrate Linux system administration
CO3	Formulate Security features for an operatingsystem
CO4	Perform memory management in OS
CO5	Implement Trust model for Multics system

REFERENCES:

1. AbrahamSilberschatz,PeterBaerGalvinandGregGagne,“OperatingSystemConcepts”,JohnWiley &Sons,Inc.,9thEdition,2012.
2. TrentJaeger,“OperatingSystemsSecurity”,Morgan&ClaypoolPublishers,2008.
3. TomAdelsteinandBillLubanovic,“LinuxSystemAdministration”,O'ReillyMedia,Inc.,1stEdition,2007.
4. WilliamStallings,“OperatingSystem:InternalsandDesignPrinciples”,PrenticeHall,7thEdition,2012.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**3**	**1**	**3**
2.	**3**	**1**	**3**
3.	**3**	**1**	**3**
4.	**3**	**1**	**3**
5.	**3**	**1**	**3**

CF22103 **NETWORK PRINCIPLES AND SECURITY**

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

1. Identify the basic networking principles
2. Understand the need for network security
3. Expose them selves to security at various network layers

UNIT I FUNDAMENTALS OF NETWORKS **9**

Networking Technology – Connecting Devices - The OSI Model - TCP/IP Model - Threats to Network communications -Wireless Network Security – Denial of Service – Distributed Denial of Service

UNIT II CRYPTOGRAPHY IN NETWORK SECURITY **9**

Malicious vs Non Malicious code – Counter Measures – Authentication – Access Control –Network and Browse Encryption–Firewalls–IDS–Network Management

UNIT III NETWORK AND TRANSPORT LAYER SECURITY **9**

Network Layer: IPSec Protocol – IP Authentication Header – IP ESP – VPN - Key Management Protocol for IPSec–Transport Layer : SSL Protocol – TLS Protocol

UNIT IV E–MAIL AND WEB SECURITY **9**

Pretty Good Privacy–MIME–S/MIME-Enhanced Security Services for S/MIME-SET for E-commerce Transactions

UNIT V CLOUD AND WIRELESS NETWORK SECURITY **9**

Cloud Computing–Cloud Security Risks and Counter Measures –Cloud Security as a Service – Wireless Network Security : Wireless Security – Mobile Device Security –WLAN Security

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Classify and secure various layers of networks
CO2	Understand the concept of Network Layer Security
CO3	Develop protocols for Web and Mail security
CO4	Apply various password management techniques for system security
CO5	Develop measures for cloud and wireless network security

REFERENCES:

1. ManYoungRhee,“InternetSecurity:CryptographicPrinciples”,“AlgorithmsandProtocols”,WileyPublications,2003.
2. CharlesPfleeger,”SecurityinComputing”,PrenticeHall,4thEdition,2006.
3. WilliamStallings,“Cryptography and NetworkSecurity”, Pearson Education,6thEdition,2013.
4. CharlieKaufman, Radia Perlman, MikeSpeciner, “NetworkSecurity”, PrenticeHall, 2ndedition ,2002.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**2**	**1**	**3**
3.	**3**	**1**	**3**
4.	**3**	**1**	**3**
5.	**3**	**1**	**3**

L	T	P	C
3	0	0	3

CF22104 COMPUTER FORENSICS AND DIGITAL EVIDENCE

COURSE OBJECTIVES:

1. Study the procedure for forensic investigation
2. Audit and analyze the computer systems for data extraction
3. Understand the process of cloud and mobile device forensics

UNIT I COMPUTER FORENSICS FUNDAMENTALS 9

Introduction to Computer Forensics – Computer Forensics Services – Benefits of ProfessionalForensics Methodology – Steps taken by Computer Forensics Specialists – Types of ComputerForensics System: IDS, Firewall – PKI – Wireless Network Security – Identity Management Security System–Identity Theft.

UNIT II COMPUTER FORENSICS TECHNOLOGY 9

Types of Military, Business and Law Enforcement Computer Forensic Technology – Specialized Forensics Techniques – Hidden Data and How to Find it – Spyware and Adware – Encryption Methods – Internet Tracing Methods – Avoiding Pitfalls with Firewall – Biometric Security Systems.

UNIT III DATA ACQUISITION AND PROCESSING CRIME SCENES 12

Understanding Storage Formats for Digital Evidence-Determining the Best Acquisition Method - Using Acquisition Tools - Validating Data Acquisitions-Performing RAID Data Acquisitions - Identifying Digital Evidence - Collecting Evidence in Private -Sector Incident Scenes - Processing Law Enforcement Crime Scenes - Preparing for a Search - Securing a Computer Incident or Crime Scene - Seizing Digital Evidence at the Scene -Obtaining a Digital Hash.

UNIT IV NETWORK AND E–MAIL FORENSICS 9

Performing Live Acquisitions - Network Forensics Overview - Exploring the Role of E-mail inInvestigations - Exploring the Roles of the Client and Server in E-mail - Investigating E-mailCrimes and Violations - Understanding E-mail Servers - Using Specialized E-mail ForensicsTools.

UNIT V CLOUD AND MOBILE DEVICE FORENSICS 6

An Overview of Cloud Computing - Legal Challenges in Cloud Forensics - Technical Challengesin Cloud Forensics - Acquisitions in the Cloud - Tools for Cloud Forensics - Understanding Mobile Device Forensics

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Plan and prepare for all stages of an investigation
CO2	Explore web server attacks, DNS and router attacks
CO3	Identify various evidences of cyber crime
CO4	Examine network traffic and identify illicit servers
CO5	Acquire data from mobile devices and crime scenes securely

REFERENCES:

1. BillNelson,AmeliaPhillips,ChristopherSteuart,“GuidetoComputerForensics andInvestigations:ProcessingDigitalEvidence”,5thedition,CengageLearning ,2015.
2. JohnR.Vacca,“ComputerForensics”,CengageLearning,2005.
3. Nelson,Phillips,Enfinger,Steuart,“ComputerForensicsandInvestigations”,CengageLearning,IndiaEdition,2008.
4. MarjieT.Britz,“ComputerForensicsandCyberCrime:AnIntroduction”,3rdEdition,PrenticeHall,2013.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**2**	**3**
2.	**2**	**2**	**3**
3.	**2**	**2**	**3**
4.	**2**	**2**	**3**
5.	**2**	**2**	**3**

GR22251 INTRODUCTION TO RESEARCH METHODOLOGY AND IPR

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

To impart knowledge on formulation of research problem, research methodology, ethics involved in doing research and importance of IPR protection**.**

UNIT I RESEARCH METHODOLOGY 6

Meaning of research problem, Sources of research problem, Criteria Characteristics of a good research problem, Errors in selecting a research problem, Scope and objectives of research problem. Approaches of investigation of solutions for research problem, data collection, analysis, interpretation, Necessary instrumentations. Effective literature studies approaches, analysis Plagiarism, Research ethics

UNIT II RESULTS AND ANALYSIS 6

Importance and scientific methodology in recording results, importance of negative results, different ways of recording, industrial requirement, artifacts versus true results, types of analysis (analytical, objective, subjective) and cross verification, correlation with published results, discussion, outcome as new idea, hypothesis, concept, theory, model etc.

UNIT III TECHNICAL WRITING 6

Effective technical writing, how to write report, Paper Developing a Research Proposal, Format of research proposal, a presentation and assessment by a review committee

UNIT IV INTELLECTUAL PROPERTY RIGHTS 6

Nature of Intellectual Property: Patents, Designs, Trade and Copyright. Process of Patenting and Development: technological research, innovation, patenting, development. International Scenario: International cooperation on Intellectual Property. Procedure for grants of patents, Patenting under PCT.

UNIT V PATENT RIGTS AND NEW DEVELOPMENTS IN IPR 6

Scope of Patent Rights. Licensing and transfer of technology. Patent information and databases. Geographical Indications. New Developments in IPR: Administration of Patent System. New developments in IPR; IPR of Biological Systems, Computer Software etc. Traditional knowledge Case Studies, IPR and IITs.

TOTAL: 30 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	***CO statements***
CO1	Critically evaluate any research article based upon research methodology.
CO2	Correlate the results of any research and develop hypothesis, concept, theory and model.
CO3	Developing a research proposal, research presentation and review article in the field of engineering.
CO4	Enumerate the importance of intellectual property right in research.
CO5	Develop proposal for patent rights and identify the new developments in IPR

TEXT BOOKS:

1. Ranjit Kumar, Research Methodology- A step by step guide for beginners, Pearson Education, Australia, fourth edition, 2014
2. Ann M. Korner, Guide to Publishing a Scientific paper, Bioscript Press 2008
3. T. Ramappa, “Intellectual Property Rights Under WTO”, S. Chand, 2008

REFERENCES:

1. Kothari, C. R. Research Methodology - Methods and Techniques, New Age International publishers, New Delhi, fourth edition, 2019
2. Stuart Melville and Wayne Goddard, “Research methodology: an introduction for science & engineering students’, Juta & Company, 1996.
3. Robert P. Merges, Peter S. Menell and Mark A. Lemley, “Intellectual Property in New Technological Age”, Aspen Publishers, 2016.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**2**	**3**
2.	**2**	**2**	**3**
3.	**2**	**2**	**3**
4.	**2**	**2**	**3**
5.	**2**	**2**	**3**

CF22111 NETWORK DESIGN AND SECURITY LABORATORY

L	T	P	C
0	0	3	2

COURSE OBJECTIVES:

1. Understand the basics of Networking
2. Learn network programming in Linux using C/Python

List of Exercises

I Network Design using CISCO Packet Tracer

1. Configure a LAN with a switch / hub with minimum 3 PCs
2. Configure a internetwork with 2 routers and two or more LANs using static routes
3. Establish a dynamic routing based internetwork with 2 routers and two or more LANs using RIP/OSPF
4. Analyze the performance of various TCP variants using an FTP application for the given network

II Network Programming using C/Python

5. Develop a program for demonstrating interprocess communication
6. Creation of TCP client/server application
7. Creation of UDP client/servera pplication
8. Develop an Iterative UDP server with 2 or 3 clients
9. Develop a concurrent TCP server with 2 or 3 clients
10. Implement Digital Signature
11. Implement ARP and RARP
12. Create a Socket based application in Python
13. Intrusion Detection using Snort tool
14. Create an application that interacts with e-mail servers in python
15. Develop applications that work with remote servers using SSH, FTP etc in Python
16. Simulate PING and TRACEROUTE commands

Total Hours:45 Periods

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Design and Configure LAN’s
CO2	Create simple network applications using C/Python
CO3	Demonstrate Interprocess communication
CO4	Simulate IDPS
CO5	Develop applications that work with remote servers

LISTOFEQUIPMENTFORABATCHOF18 STUDENTS

SOFTWARE:

Windows/Ubuntu/KaliLinuxwithC/C++/Java/PythonCiscoPacketTracer,SnortIDS,EclipseorequivalentIDE

HARDWARE:

Standalonedesktops-18

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**2**	**1**	**3**
3.	**3**	**1**	**3**
4.	**3**	**1**	**3**
5.	**3**	**1**	**3**

CF22112 ETHICAL HACKING ESSENTIALS LABORATORY

L	T	P	C
0	0	3	2

COURSE OBJECTIVES:

1. Understand the basics of Ethical Hacking
2. Learn various Hacking tools

List of Exercise

1. Basic Linux Commands
2. Advanced Linux commands
3. Information Gathering
4. Vulnerability Analysis
5. Web Application Analysis
6. Database Assessment
7. Password Attacks
8. Wireless Attacks
9. Reverse Engineering
10. Exploitation tools
11. Sniffing & spoofing
12. VM-WARE

TotalHours:45 Periods

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Gather the information from various sources
CO2	Assess the vulnerabilities in Database
CO3	Analyse the vulnerabilities in Web application
CO4	Enumerate various attacks and its countermeasures
CO5	Use different Exploitation tools

LISTOFEQUIPMENTFORABATCHOF18STUDENTS:

SOFTWARE:

KaliLinuxanditsTools

HARDWARE:

Standalonedesktops-18

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	2	3
2.	2	2	3
3.	2	2	3
4.	2	2	3
5.	2	2	3

CF22201 FUNDAMENTALS TO SECURITY IN BIOMETRICS

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

The students will be able to

1. Understand the functionalities of biometrics
2. Discover the need of biometrics for an organization
3. Learn to develop biometric based applications
4. Emphasize the need of biometric security

UNIT I FUNDAMENTALSOF BIOMETRICS 9

Biometric System–Enrollment and recognition–Sensor modules–Feature extraction module - Database module–Matching module–Biometric functionalities–Biometric system errors– Design cycle of Biometrics–Security and Privacy issues.

UNIT II FINGERPRINTRECOGNITION 9

Friction ridge pattern : Features and formation–Fingerprint Acquisition–Feature extraction– Matching–Fingerprint indexing–Fingerprint synthesis: Level1 and Level2–Palmprint.

UNIT III FACEANDIRISRECOGNITION 9

Psychology of face recognition–Facialfeatures–Design–Image acquisition–Face detection - Feature extraction and matching–Face modelling–Iris Recognition: Design and Image acquisition – Image segmentation – Image normalization, Encoding and matching –Iris quality - Performance Evaluation.

UNIT IV SIGNATUREANDKEYSTROKERECOGNITION 9

Behavioural biometrics – Features and Classification –Signature Recognition : History of Handwriting Analysis- Automated Systems for Signature Recognition- Offline and Online Signatures- Types of Forgeries- Databases for Signature System Evaluation - Commercial Software – Signature Recognizers – Keystroke Dynamics: Keystroke Analysis - Authentication and Identification-Characteristics of Keystroke Dynamics - Approaches to Keystroke Dynamics.

UNIT V SECURITYINBIOMETRICS 9

Adversary Attacks – Insider and Infrastructure attack - Attacks at the User Interface – Impersonation – obfuscation – spoofing - Counter measure: spoofdetection -Attacks on Biometric Processing – System modules and interconnections-Attacks on theTemplate Database - Biometric template security.

TOTAL: 45 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Identify various biometric techniques
CO2	Design biometric recognition systems
CO3	Develop simple biometric based application
CO4	Elucidate the need for biometric security
CO5	Analyse the various attacks possible in Biometric system

References

1. Jameswayman,Anilk.Jain,ArunA.Ross,KarthikNandakumar,“IntroductiontoBiometrics”,Springer, 2011.
2. KhalidsaeedwithMarcinAdamski,“NewDirectionsinBehavioralBiometrics”,CRC Press2017
3. PaulReid"BiometricsForNetworkSecurity",PersonEducation2004.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**2**	**3**
2.	**3**	**2**	**3**
3.	**3**	**2**	**3**
4.	**2**	**2**	**3**
5.	**2**	**2**	**3**

CF22202 DIGITAL FORENSICS AND DIGITAL INVESTIGATIONS

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

The students will be able

1. To understand the basic digital forensics and techniques for conducting the forensic examination on different digital devices.
2. To understand how to examine digital evidences such as the data acquisition, identification analysis.

UNIT I DIGITAL FORENSICS 9+3

Foundations of Digital Forensics - Digital Evidence - Increasing Awareness of Digital Evidence -Digital Forensics: Past, Present, and Future -Principles and Challenges of Digital Forensics - Digital Forensics Research - Language of Computer Crime Investigation.

UNIT II DIGITAL INVESTIGATIONS 9+3

Conducting Digital Investigations -Digital Investigation Process Models -Scaffolding for Digital Investigations - Applying the Scientific Method in Digital Investigations -Fundamental Principles - Preparing to Handle Digital Crime Scenes – Surveying and Preserving the Digital Crime Scene - Equivocal Forensic Analysis – Victimology - Crime Scene Characteristics.

UNIT III DIGITAL EVIDENCE 9+3

Violent Crime and Digital Evidence - Digital Evidence as Alibi - Investigating an Alibi– Time and Location as Alibi - Investigating Computer Intrusions - Forensic Preservation of Volatile Data - Investigation of Malicious Computer Programs – Cyberstalking.

UNIT IV COMPUTERBASICSFORDIGITALINVESTIGATORS 9+3

Basic Operation of Computers - Representation of Data - File Systems and Location of Data -Dealing with Password Protection and Encryption - Applying Forensic Science to Computers -Digital Evidence on Windows Systems- Digital Evidence on UNIX Systems.

UNIT V FORENSIC SCIENCE ON NETWORKS 9+3

Digital Evidence on the Internet - Online Anonymity and Self-Protection - E-mail Forgery andTracking - Usenet Forgery and Tracking - Digital Evidence on Physical and Data-Link Layers -Digital Evidence at the Network and Transport Layers.

TOTAL(L:45+T:15): 60 PERIODS

OUTCOMES:

Upon successful completion of the course, students should be able to:

CO	*CO statements*
CO1	Relate the fundamentals of computer forensics, laws, report writing and tools in digital investigations.
CO2	Assess the investigative smart practices and applicability of concerned laws & investigative tools
CO3	Inspect the acquired data, recover the deleted data and manage a case .
CO4	Select the correct method to handle the digital evidence and acquire appropriate certification to build the career in digital forensics.
CO5	Create a method for gathering, assessing and applying new and existing legislation specific to the practice of digital forensics.

References

1. EoghanCasey,“DigitalEvidenceandComputerCrimeForensicScience,ComputersandtheInternet”,ThirdEdition,Elsevier,2011
2. KevinMandia,ChrisProsise,MattPepe,―IncidentResponseandComputerForensics―, TataMcGraw -Hill,NewDelhi,2006.
3. NelsonPhillipsandEnfingerSteuart,―ComputerForensicsandInvestigations‖,Cengage Learning,New Delhi,2009.
4. CoryAltheideandHarlanCarvey,―DigitalForensicswithOpenSourceTools‖Elsevierpublication,April2011

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**2**	**3**
2.	**2**	**2**	**3**
3.	**2**	**2**	**3**
4.	**2**	**2**	**3**
5.	**2**	**2**	**3**

CF22203 BLOCKCHAIN FOR SECURITY

L	T	P	C
3	0	0	3

COURSE OBJECTIVES:

The students will be able to

1. Understand the cryptography basics of a blockchain
2. Recognize the requirement of a simple blockchain application
3. Study about the tools used for blockchain development

UNIT I CRYPTO FUNDAMENTALS FOR BLOCKCHAIN 12

Hash Functions–Digital Hash–Pre-image resistance–Second pre-imageresistance–Message Digest–Secure Hash Algorithms–Distributed HashTables–Digital Signatures–Signcryption–Blind Signatures.

UNIT II FEATURES OF BLOCKCHAIN 9

History of Blockchain–Decentralization–Generic Elements of Blockchain–Addresses – Transaction – Block – Contents of a Block – Block Header - State Machine – Nodes–Types of Blockchain.

UNIT III CONSENSUSIN BLOCKCHAIN 9

Fault tolerance–Paxos–Consensus–Byzantine Agreement–Proof of Work–Proof of Stake – Proof of Elapsed Time–Proof of Importance–Practical Byzantine Fault Tolerance–CAP Theorem-Mining –How blockchain accumulates block.

UNIT IV HYPERLEDGER FORBLOCKCHAIN 9

Hyperledger as a protocol – Fabric – Sawtooth lake – Reference Architecture – Privacy and Confidentiality – Fabric Architecture – Components of the fabric – Blockchain services – API'sandCLI's.

UNIT V APPLICATIONS OF BLOCKCHAIN 9

Bitcoin – Crypto currency–Smart Contracts – Financial Applications–IoT Blockchain Applications – Government Applications – Blockchain Security.

TOTAL: 45 PERIODS

OUTCOMES:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Elucidate the requirements of a blockchain
CO2	Design a simple blockchain based application
CO3	Implement Consensus mechanism in blockchain
CO4	Deploy sample applications over Hyperledger
CO5	Explain the requirement of mining in blockchain

References

1. ImranBashir,“MasteringBlockchain”,PacktPublishing2017.
2. MelanieSwan,“Blockchain-BlueprintforaNewEconomy”,O'ReillyMedia,2015
3. RogerWattenhofer,“Thescienceoftheblockchain”,InvertedForestPublishing,2016
4. www.blockchain.io
5. www.blockchain.org

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**2**	**1**	**3**
3.	**3**	**1**	**3**
4.	**3**	**1**	**3**
5.	**3**	**1**	**3**

CF22204 INTERNET OF THINGS AND SECURITY

L	T	P	C
3	1	0	4

COURSE OBJECTIVES:

The students will be able to

1. Understand the fundamentals of Internet of Things
2. Fabricate a low cost embedded system using Raspberry Pi or Arduino
3. Apply IoT in Real world scenario

UNIT I FUNDAMENTALSOFIOT 12

The flavour of the Internet – Technology of IoT – Enchanted objects – Design principles for connected device–Privacy–Web thinking– Affordance.

UNIT II INTERNETPRINCIPLES 12

Internet Communications– IP,TCP – Protocol suite– UDP – IP Addresses– TCP and UDP ports– MAC Address– Application Layer Protocols.

UNIT III PROTOTYPINGEMBEDDEDDEVICES 12

Prototypes and production - Open source versus closed source - Tapping into the community –Electronics-Embedded computing basics–Arduino - Raspberry pi-electric imp–plug computing.

UNIT IV PROTOTYPINGPHYSICALANDONLINECOMPONENTS 12

Preparation, sketch, iterate and explore - Non digital methods - Laser cutting - 3D printing –Getting started with API – Writing a new API – Real time reactions–Memory Management.

UNIT V PROTOTYPETOBUSINESS MODELS 12

Business model canvas – Models - Funding an internet of things startup – Scaling up Software –Ethics:Privacy –Control–Environment–Solutions

TOTAL: 60 PERIODS

OUTCOMES:

At the end of the course, the students will be able to,

CO	***CO statements***
CO1	Analyze various protocols of IoT
CO2	Design a portable IoT application using Raspberry Pior Arduino
CO3	Deploy an IoT application to the cloud.
CO4	Analyze applications of IoT in realtime scenario
CO5	Design Prototype for physical and online components

References

1. AdrianMcEwen,HakimCassimally,DesigningtheInternetofThings,1/e,Wileypublication,2013
2. CharalamposDoukas,BuildingInternetofThingswiththeArduino,Createspace,2002.
3. DieterUckelmann(et.al),ArchitectingtheInternetofThings,Springer,2011.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22211 IOT AND BLOCKCHAIN LABORATORY

L	T	P	C
0	0	3	2

CourseObjectives:

The students will be able to

1. Understand the basics of Arduino / Raspberry Pi programming
2. Learn to develop simple blockchain applications.

Arduino and RaspberryPi

1. Arduino programming to make the LED Blink with and without delay
2. Serial Communication in Arduino with Wireless Module and Programming
3. Bluetooth (HC-05) and ZigBee (TI-CC2500)
4. Programming the Raspberry Pi to make the LED Blink using Python
5. Integration of sensors / components with Raspberry Pi and Programming
6. Serial Communication Between Arduino and Raspberry Pi using Universal Serial Bus(USB)

Security in Arduino and RaspberryPi

7. Implementation of MD5, SHA1, SHA256 in Arduino / Raspberry Pi using Hash Functions.
8. Implementation of DES and AES Algorithms in Arduino / Raspberry Pi using Arduino Cryptographic Library.

Blockchain Implementation

9. Implementation of basic Hash algorithms required for Blockchain
10. Developing simple applications using Hyperledger framework
11. Developing simple applications using Ethereum framework
12. Simulation of mining in Blockchain
13. Implementation of ethereum smart contracts

Total Hours:45 Periods

Course Outcomes:

At the end of the course, the students will be able to,

CO	***CO statements***
CO1	Develop simple applications using Arduino / RaspberryPi
CO2	Implement various security protocols
CO3	Create simple applications using blockchain tools
CO4	Simulate mining in blockchain

LISTOFEQUIPMENTFORABATCHOF18STUDENTS:

SOFTWARE:

Windows/Ubuntu/KaliLinuxwithC/C++/Java/PythonCiscoPacketTracer,SnortIDS,EclipseorequivalentIDE

HARDWARE:

Standalonedesktops–18 IoT kit -18

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22212 DIGITAL FORENSICS LABORATORY

L	T	P	C
0	**0**	**3**	**2**

Course Objectives:

The students will be able to

1. Perform basic digital forensics.
2. Demonstrate the use of simple digital forensics tools.
3. Conduct a digital forensics exercise.

List of Exercises

Disk Imaging and Cloning

1. Use VMWare and modify device configuration in a VMWare system

Analyzing disk structure and file systems

2. The Sleuth Kit Tools

Search Word Filtering from Unallocated, Slack and Swap Space Unix File Recovery – Data Unit Level

3. Review of unallocated space and extracting with dls

FILE RECOVERY : META DATALAYER

4. Find meta data information for evidence found in a searchlist

Keyword Searches, Timelines, HiddenData

DataMiningforDigitalForensics

5. Encryption and Password Recovery
6. Steganography Detection
7. File Extension Renaming and Signaturing
8. Application Analysis
9. Client and Web Analysis
10. Network Analysis

Total Hours:45

CourseOutcomes:

At the end of the course,the students will be able to,

CO	*CO statements*
CO1	Practice and gain basic knowledge about VM ware and various file system
CO2	Analyse disk structure and file system
CO3	Perform file recovery
CO4	Perform mining for digital forensics
CO5	Apply steganography in digital forensics

LIST OF EQUIPMENT FOR A BATCH OF 18 STUDENTS:

SOFTWARE:

Ubuntu / Kali Linux with C/C++/Java/PythonSleuth Kit, Wireshark, VMWare, OWASP, DVWA

HARDWARE:

Standalone desktops - 18

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22002 PENETRATION AND APPLICATION TESTING

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand and analyse entire penetration testing process including planning , reconnaissance , scanning, exploitation, post-exploitation, and result reporting
- To understand the fundamental information associated with methods employed and in securities identified
- To develop an excellent understanding of current cyber security issues and ways that user , administrator , and programmer errors can lead to exploitable insecurities.

UNIT I THE BASICS 9

Using Kali Linux–Linux File System–User Privilege–File permission–Data manipulation – Managing and Networking – Shell and python Scripting – Metasploit Framework

UNIT II ASSESSMENTS AND EXPLOITATION 9

Finding Vulnerabilities – Nmap scripting engine – Metasploit Scanner –Metasploit exploit check functions Webapplication scanning – Using wireshark to capture traffic – SSL attacks and scripting – Exploiting Web Dav credentials –Exploiting Open php My Admin – Exploiting third party web appplications

UNIT III EXPLOITDEVELOPMENT 9

Stack based buffer overflow in Linux – Memory Theory – Linux Buffer overflow - Stack based buffer over flow in Windows–Causing crash–Locating EIP–Structured exception handler – Fuzzing programs Porting public exploits–Writing metasploit modules–Exploitation mitigation techniques

UNIT IV POSTEXPLOITATION 9

Client side exploitation – Bypassing filters – Client side attacks – Social Engineering – Bypassing Antivirus applications–Meterpreter–Local information gathering–Lateral movement – Pivoting – Persistence –Web Application testing – SQL injection–Xpath injection – Crosssite scripting -Web application scanning with w3af.

UNITV WIRELESS ANDMOBILEHACKING 9

Monitoring mode – Wired equivalent privacy – WPA2 – Wifi protected setup–Smartphone pentest framework – Mobile attack vectors – Remote and Clientside attacks–Malicious apps–Mobile post exploitation.

TOTAL:45 PERIODS

Course Outcomes:

At the end of the course, the students will be able to,

CO	***CO statements***
CO1	Demonstrate professional and ethical responsibility , communicate effectively, the impact of security practices in a global and societal context
CO2	Elaborate vulnerabilities, mechanisms to identify vulnerabilities / threats / attacks
CO3	Apply knowledge of engineering to security evaluations, design and conduct security assessment experiments
CO4	Apply techniques and modern engineering tools necessary for computer security engineering practice
CO5	Enumerate the technical workings of various penetration tests and produce reports based on them

References

1. Georgia Weidman, Penetration Testing– A hands -on introduction to hacking, No Scratch Press, 2014
2. JonErickson,Hacking:TheArtofExploitation,O’Reilly2ndEdition
3. RajatKhare,"NetworkSecurityandEthicalHacking",LuniverPress,2006
4. RamachandranV,BackTrack5WirelessPenetrationTestingBeginner’sGuide(3rd ed.).PacktPublishing,2011
5. ThomasMathew,"EthicalHacking",OSBpublishers,2003

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22004 APPLIED CRYPTOGRAPHY

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

1. Understand basic encryption methods and algorithms, strengths and weaknesses of encryption algorithms.
2. Understand encryption key exchange and management
3. Gain knowledge on hashing and its applications

Unit I Cryptography and Computational Hardness 9

Introduction -Private Key Cryptography - Public Key Cryptography - Hash functions - Digital Signature - Multiplication, Primes, and Factoring - Hardness Amplification - Collections of One-Way Functions - Basic Computational Number Theory - Factoring-based Collection of OWF-Discrete Logarithm-based Collection

Unit II Indistinguishability and Pseudo-Randomness 9

RSA Collection - One-way Permutations - Trapdoor Permutations - Rabin collection-AUniversal One Way Function - Computational Indistinguishability - Pseudo-random generators - Hard-Core Bits from Any OWF- Secure Encryption - An Encryption Scheme with Short Keys - Multi-message Secure Encryption - Pseudorandom Functions - Construction of Multi-message Secure Encryption-Public Key Encryption-El-Gamal Public Key Encryption scheme-A Note on Complexity Assumptions

Unit III Public Key and Private Key Cryptosystems 9

Chosen plaintext attack - Security against multi-key attacks - Building CPA secure ciphers -Nonce based encryption - Message integrity - Message integrity from Universal Hashing -Elliptic Curve cryptography and pairings-Analysis of number theoretic assumptions

Unit IV Protocols for Cryptography 9

Protocols for Identification and Login - Authenticated Encryption -Identification and signatures from sigma protocols - Combining Sigma protocols - Witness independence and applications-Proving properties in zero - knowledge

Unit V Protocols for Key Exchange 9

Authenticated Key exchange - HSM security -One-sided Authentication - Deniability - Password authenticated key exchange - Secure multi - party computation -Evaluating arithmetic circuits - Garbled circuits - Formal models for multiparty communication

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Design algorithms for constructing cryptographic computations
CO2	Analyse the correctness of cryptographic protocols.
CO3	Enumerate the methods used for encryption , authentication, integrity, certification and data privacy.
CO4	Apply the complex protocols that involve many steps and computing agents, who do not trust eachother.
CO5	Simulate the electronic transactions

References

1. Rafael Pass and AbhiShelat, “A Course in Cryptography”,Thirdedition:January2010
2. Dan Bonehand VictorShoup,“A Graduate Course in Applied Cryptography”, January2020.
3. WilliamStallings,“Cryptography and Network Security: Principles and Practices”, Seventh Edition,Pearson Education,2017.
4. MattBishop,“Computer Security art and science”, Second Edition, Pearson Education, 2002

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22005	**MACHINE LEARNING TECHNIQUES**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives :

The students will be able to

1. To introduce students to the basic concepts and techniques of Machine Learning.
2. To have a thorough understanding of the Supervised and Unsupervised learning techniques.
3. To study the various probabilities based learning techniques.

Unit I Introduction to Machine Learning Techniques 9

Learning – Types of Machine Learning – Supervised Learning – The Brain and the Neuron –Design a Learning System – Perspectives and Issues in Machine Learning – Concept Learning Task – Concept Learning as Search – Finding a Maximally Specific Hypothesis – Version Spaces and the Candidate Elimination Algorithm–Linear Discriminants – Perceptron – Linear Separability–Linear Regression.

Unit II Linear Models 9

Multi-layer Perceptron– Going Forwards–Going Backwards: Back Propagation Error– Multilayer Perceptron in Practice – Examples of using the MLP – Overview – Deriving Back Propagation – Radial Basis Functions and Splines–Concepts–RBF Network–Curse of Dimensionality –Interpolations and Basis Functions–Support Vector Machines.

Unit III Tree and Probabilistic Models 9

Learning with Trees – Decision Trees – Constructing Decision Trees –Classification and Regression Trees – Ensemble Learning – Boosting – Bagging – Different ways to Combine Classifiers – Probability and Learning – Data into Probabilities – Basic Statistics – Gaussian Mixture Models – Nearest Neighbor Methods – Unsupervised Learning–Kmeans Algorithms Vector Quantization–Self Organizing Feature Map.

Unit IV Dimensionality Reduction and Evolutionary Models 9

Dimensionality Reduction – Linear Discriminant Analysis – Principal Component Analysis –Factor Analysis – Independent Component Analysis – Locally Linear Embedding – Isomap –LeastSquaresOptimization–EvolutionaryLearning–Geneticalgorithms–GeneticOffspring:- Genetic Operators – Using Genetic Algorithms – Reinforcement Learning – Overview – Getting Lost Example–Markov Decision Process.

Unit V Graphical Models 9

Markov Chain Monte Carlo Methods – Sampling – Proposal Distribution – Markov Chain MonteCarlo – Graphical Models – Bayesian Networks – Markov Random Fields – Hidden Markov Models– Tracking Methods.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Distinguish between, supervised, unsupervised and semi-supervised learning
CO2	Apply the apt machine learning strategy for any given problem
CO3	Suggest supervised, unsupervised or semi-supervised learning algorithms for given problem
CO4	Design systems that uses the appropriate graph models of machine learning

References

1. EthemAlpaydin,"IntroductiontoMachineLearning3e(AdaptiveComputationand MachineLearningSeries)",ThirdEdition,MIT Press,2014
2. JasonBell,"Machinelearning–Hands on for Developers and Technical Professionals", FirstEdition, Wiley, 2014
3. PeterFlach,"Machine Learning: The Art and Science of Algorithms that MakeSense of Data", FirstEdition, Cambridge University Press,2012.
4. Stephen Marsland,"Machine Learning– An Algorithmic Perspective", Second Edition, Chapman and Hall, CRC Machine Learning and Pattern Recognition Series, 2014.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22006	DATA MINING TECHNIQUES	L	T	P	C
		3	0	0	3

Course Objectives:

The students will be able to

1. Understand Data mining principles and techniques and Introduce DM as a cutting edge business intelligence
2. Explore the concepts of Dataware housing Architecture and Implementation
3. Study the overview of developing areas– Webmining, Text mining and ethical aspects of Datamining
4. Identify Business applications and Trends of Datamining

UnitI Introduction to Data Warehousing 9

Evolution of Decision Support Systems - Dataware housing Components–Building a Datawarehouse, DataWarehouse and DBMS, Datamarts, Metadata, Multidimensional datamodel, OLAP vs OLTP, OLAP operations, Data cubes, Schemas for Multidimensional Database:Stars,Snowflakes and Fact constellations

UnitII Data Warehouse Process and Architecture 9

Types of OLAP servers, 3–Tier data ware house architecture, distributed andvirtualdatawarehouses. Data warehouse implementation, tuning and testing of data warehouse. Data Staging(ETL) Design and Development, data warehouse visualization, Data Warehouse Deployment,Maintenance,Growth,BusinessIntelligenceOverview-DataWarehousing and Business Intelligence Trends-Business Applications-tools-SAS

UnitIII Introduction to DataMining 9

Data mining-KDD versus datamining, Stages of the Data Mining Process-task premitives, DataMining Techniques -Data mining knowledge representation–Datamining querylanguages,Integration of a Data Mining System with a Data Warehouse – Issues, Data preprocessing – Datacleaning, Data transformation, Feature selection, Dimensionality reduction, Discretization and generating concept hierarchies-Mining frequent patterns-association-correlation

UnitIV Classification and Clustering 9

DecisionTree Induction - Bayesian Classification – RuleBasedClassification – Classificationby Backpropagation – Support Vector Machines – Associative Classification – Lazy Learners –Other Classification Methods –Clustering techniques – ,Partitioning methods - k-means - Hierarchical Methods– distance based agglomerative and divisible clustering, Density-Based Methods – expectation maximization-GridBased Methods–Model-Based Clustering Methods- Constraint –Based ClusterAnalysis – Outlier Analysis

UnitV Predictive Modeling Of BigData and Trends In Datamining 9

Statistics and Data Analysis – EDA – Small and Big Data –Logistic Regression Model – OrdinaryRegression Model-Mining complex data objects –Spatial databases – Temporal databases –Multimediadatabases–Timeseriesandsequencedata–Textmining–Webmining–Applicationsin Datamining

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Design Multidimensional Intelligent model from typical system
CO2	Explore the features of high dimensional system
CO3	Implement various mining techniques on complex data objects
CO4	Apply various Business Applications Tools
CO5	Analyze various classification and clustering techniques

References

1. Jiawei Han, Micheline Kamber, DataMining: Concepts and Techniques, Morgan Kaufmann Publishers,thirdedition2011,ISBN:1558604898.
2. AlexBersonand StephenJ.Smith,“ Data Warehousing, Data Mining &OLAP ”, TataMcGrawHillEdition,TenthReprint 2007.
3. G. K. Gupta, “Introduction to Data Min Data Mining with Case Studies”, Easter EconomyEdition,PrenticeHallofIndia,2006.
4. Data Mining:Practical Machine Learning Tools and Techniques,Third edition,(Then MorganKufmann series in Data Management systems), Ian.H.Witten, Eibe Frank and Mark.A.Hall,2011
5. Statistical and Machine learning –Learning Data Mining, techniques for better PredictiveModelingand AnalysistoBigData

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22007 INTRUSION DETECTION AND PREVENTION SYSTEMS

		L	T	P	C
CF22007	INTRUSION DETECTION AND PREVENTION SYSTEMS	3	0	0	3

Course Objectives:

The students will be able to

1. Understand the state of the art of intrusion detection system
2. Design and implement Intrusion Detection System
3. Understand the classes of attacks on computersystems
4. Identify various types of IDS of signature based and anomaly based techniques to solve problems related to intrusion detection and prevention.

UnitI Introduction 9

Understanding Intrusion Detection – Intrusion detection and prevention basics – IDS and IPS analysis schemes, Attacks, Detection approaches – Misuse detection–anamoly detection – specification based detection– hybrid detection - methodologies-Signature & Anomaly based Detection, Stateful protocol analysis Types of IDS, Information sources Host based information sources, Network based information sources.

UnitII Theoretical Foundations of Detection Technologies 9

Taxonomy of anomaly detection system – fuzzy logic – Bayes theory–Artificial Neural networks – Support vector machine - IDS TECHNOLOGIES: Components & Architecture -Typical components, Network Architectures Security capabilities-Information gathering capabilities, logging capabilities, detection & prevention capabilities. Network protocol based IDS, Hybrid IDS,and Analysis schemes.

UnitIII Network Based IDS 9

Networking Overview - OSI layers. Components and Architecture-Typical components, Network architectures and sensor locations. Security capabilities Wireless IDPS-Wireless Networking overview -LAN standards & components. Components Network Behaviour analysis system.

UnitIV Host Based IDS 9

Components and Architecture-Typical components, Network architectures, Agent locations, host architectures. Security capabilities-Logging,detection,prevention and other capabilities. Using & Integrating multiple IDPS technologies - Need for multiple IDPS technologies, Integrating different IDPS technologies -Other technologies with IDPS capabilities, Anti-malware technologies, Firewalls and Routers, Honeypots.

UnitV Applications and Snort Tools 9

Tool Selection and Acquisition Process - Intrusion Detection–Prelude Intrusion Detection -Cisco Security IDS - Snorts Intrusion Detection – NFR security -Introduction to Snort, Working with Snort Rules, Snort configuration, Snort with MySQL, Running Snort on Multiple Network Interfaces.

Total Hours:45

CourseOutcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Enumerate the need of anomaly detection and its types
CO2	Analyze various IDS technologies
CO3	Configure a network using IDS tools
CO4	Configure a server and its hosts for real time Intrusion Detection
CO5	Select and install a IDS system such as Snort to secure the network

References

1. CarlEndorf,EugeneSchultzandJimMellander"IntrusionDetection&Prevention",1stEdition,TataMcGraw-Hill,2006
2. AliA.Ghorbani,WeiLu,"NetworkIntrusionDetectionandPrevention:ConceptsandTechniques",Springer,2010.
3. KarenScarfone,PeterMell,"GuidetoIntrusionDetectionandPreventionSystems(IDPS)", NISTspecialpublication,2007.
4. StephenNorthcutt,JudyNovak:"NetworkIntrusionDetection",3rdEdition,NewRidersPublishing,2002.
5. PaulE.Proctor,"ThePracticalIntrusionDetectionHandbook",PrenticeHall,2001.
6. RafeeqRehman:"IntrusionDetectionwithSNORT,Apache,MySQL,PHPandACID,"1st Edition,Prentice Hall ,2003

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CP22008 SOCIAL NETWORK ANALYSIS L T P C
3 0 0 3

Course Objectives:

The students will be able to

1. Understand the concepts of Social networks and Web Social Networks
2. Appreciate the modelling and visualizing techniques associated with Social Networks

Unit I Social Network Analysis Fundamentals 9

Introduction to Web - Limitations of current Web – Development of Semantic Web – Emergence of the Social Web – Statistical Properties of Social Networks -Network analysis– Development of Social Network Analysis - Key concepts and measures in network analysis – Discussion networks- Blogs and online communities- Web-based networks.

Unit II Modeling and Visualization 9

Visualizing Online Social Networks - A Taxonomy of Visualizations - Graph Representation -Centrality- Clustering - Node-Edge Diagrams - Visualizing Social Networks with Matrix Based Representations- Node-Link Diagrams - Hybrid Representations - Modelling and aggregating social network data - Random Walks and their Applications –Use of Hadoop and Map Reduce -Ontological representation of social individuals and relationships.

Unit III Mining Communities 9

Aggregating and reasoning with social network data, Advanced Representations – Extracting evolution of Web Community from a Series of Web Archive - Detecting Communities in Social Networks - Evaluating Communities – Core Methods for Community Detection & Mining -Applications of Community Mining Algorithms -Node Classification in Social Networks.

Unit IV Evolution 9

Evolution in Social Networks – Framework - Tracing Smoothly Evolving Communities – Models and Algorithms for Social Influence Analysis - Influence Related Statistics-Social Similarity and Influence - Influence Maximization in Viral Marketing - Algorithms and Systems for Expert Location in Social Networks – Expert Team Formation - Link Prediction in Social Networks -Feature based Link Prediction-Bayesian Probabilistic Models - Probabilistic Relational Models.

Unit V Text and Opinion Mining 9

Text Mining in Social Networks -Opinion extraction – Sentiment classification and clustering -Temporal sentiment analysis - Irony detection in opinion mining - Wish analysis - Product review mining – Review Classification–Tracking sentiments towards topics overtime.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Build a social network data set from existing social networking sites
CO2	Identify the components of a web social network
CO3	Identify the different data structures and graph algorithms that can be used for web social network mining
CO4	Perform text and opinion mining in social network
CO5	Design Models and Algorithms for social Influence Analysis

References

1. CharuC.Aggarwal,“SocialNetworkDataAnalytics”,Springer;2011
2. PeterMika,“SocialNetworksandtheSemanticWeb”,Springer,1st edition2007.
3. Bork oFurht, “Handbook of Social Network Technologies and Applications ”, Springer, 1st edition,2010.
4. Guandong Xu, Yanchun Zhangand LinLi,“WebMiningandSocialNetworking–Techniquesandapplications”,Springer, 1st edition,2011.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22011	**PRINCIPLES OF SECURE CODING**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

The students will be able to

1. Explain security design principles
2. Analyze and Design projects by applying security principles
3. Implement projects using security primitives
4. Utilize tools for security analysis

UnitI Introduction to Security 9

Security goals- -Proactive Security development process, Secure Software Development Cycle(S-SDLC), Security issues whilewriting SRS, Best Practices SD3(Secureby design,defaultanddeployment),SecurityprinciplesandSecureProductDevelopmentTimeline ,SecurityDesignPrinciples.

UnitII Secure Programming Techniques 9

Worms and other malware, Buffer overflows, client state manipulation, sql injection-password security-cross domain security in web applications.

UnitIII Secure coding 9

Safe initialization ,Access control, Input validation, buffer overflows, format String problems,Integeroverflows,C++catastrophes,Catchingexceptions,commandinjection,informationleakage, Race conditions, Poor usability executing code with too much privilege. Failure to,protectstoreddata.

Unit IV Database and Web-specific issues 9

SQL Injection Techniques and Remedies, Race conditions, Time of Check Versus Time of Use and its protection mechanisms. Validating Input and Interprocess Communication, Securing Signal Handlers and File Operations. XSS scripting attack and its types – Persistent and Non persistent attack XSS Counter measures and By passing the XSS Filters.

Unit V Testing secure applications 9

Testing Secure Applications: Security code overview, secure software installation. The Role of the Security Tester, Building the Security Test Plan. Testing HTTP - Based Applications, Testing File-Based Applications, Testing Clients with Rogue Servers

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Elucidate the principles required for securing an organization
CO2	Create secure projects for an organization
CO3	Deploy projects and their security features
CO4	Design methodologies for secure software development
CO5	Utilize the tools available for security and secure an organization

References

1. Foundations of Security, DaswaniN., KernC.,KesavanA.,Apress
2. 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them by John Viega(Author),MattMessier(Author)
3. Secure Programming Cook book for C and C++, O'ReillyMedia
4. Writing Secure Code, Michael Howard and David LeBlanc, Microsoft Press, 2ndEdition, 2004

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	1	3
2.	3	1	3
3.	2	1	3
4.	2	1	3
5.	3	1	3

		L	T	P	C
CF22013	**TRUST MANAGEMENT IN E-COMMERCE**	**3**	**0**	**0**	**3**

Course Objectives:

The students will be able to

1. Ecommerce business models and Digital Payments systems
2. Knowledge about Ecommerce security Environment
3. To study about Ecommerce mechanisms and trusted computing Platform.

Unit I Introduction To E-Commerce 9

Introduction to E-Commerce – Network and E-Commerce – Types of E-Commerce – E-commerce Business Models, Major Business to Consumer(B2C) businessmodels ,Major Business to Business (B2B) business models, Business models in emerging E-commerce areas, How the Internet and the web change business: strategy, structure and process, The Internet: Technology Background, The Internet Today, Internet II - The Future Infrastructure.

Unit II E-Commerce Security and Payment 9

E-commerce security environment, Security threats in the e-commerce environment, Technology solution, Management policies , Business procedures, and publiclaws, Payment system, E-commerce payment system, Electronic billing presentmentand payment.

Unit III Trust InE-Commerce 9

Inter-organizational trust in E-Commerce: Need – Trading partner trust – Perceived benefits and risks of E-Commerce–Technology trust mechanismin E-Commerce– Perspectives of organizational, economic and political theories of inter-organizational trust –Conceptual model of inter-organizational trustin E-Commerce participation.

Unit IV Trusted Computing Platform 9

Introduction to trusted computing platform: Overview – Usage Scenarios – Key components of trusted platform–Trust mechanisms in a trusted platform.

Unit V Trust Models 9

Trusted platforms for organizations and individuals– Trust models and the E-Commerce domain.

TotalHours:45

CourseOutcomes:

At the end of the course, the students will be able to,

CO	***CO statements***
CO1	Explain B2C, B2B, C2C, Business models
CO2	Illustrate the Policies, Procedures and Laws and Security threats in E-Commerce environment
CO3	Analyze and explain the issues, risks and challenges in inter-organisational trust in Ecommerce
CO4	Explain the Key components and Trust mechanisms of trusted computing platform.
CO5	Describe the Trusted platforms for organizations and individuals

.

References

1. S.J.Joseph,E-Commerce:anIndianperspective,PHI
2. KennethC.LaudonandCarolGuercioTrave,—E-CommerceBusinessTechnologySociety‖,12thEditionPearsonEducation,2016.
3. PaulineRatnasingam,—Inter-OrganizationalTrustforBusiness-to-BusinessE-Commerce‖,IRMPress,2005.
4. SianiPearson,etal,—TrustedComputingPlatforms:TCPATechnologyinContext‖PrenticeHallPTR,2002.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22015	BIOMETRIC IMAGE PROCESSING	L	T	P	C
		3	**0**	**0**	**3**

Course Objectives:

The students will be able to

1. Understand the basics of Image processing
2. Model and picture the transformation of image
3. Understand the growth of object detection

Unit I Image Processing Essentials 9

Human vision system – Computer vision system – Image formation – Fourier Transform– Sampling Criteria – Histograms – Point operators – Group operations – Statistical operations –Mathematicalmorphology.

Unit II Feature Extraction : Edge detection and Fixed shape matching 9

Edge Detection- Phase congruency- Localized feature extraction- Describing image motion -Thresholding and subtraction - Template matching - Feature extraction by low-level features -Hough transform-Deformable shape analysis-Active contours(snakes).

Unit III Object Detection and Description 9

Boundary descriptions-Region descriptors-Texture description–Classification–Segmentation -Moving object detection -Tracking moving features -Moving feature extraction and description.

Unit IV Voice and Hand Biometrics 9

Voice biometric techniques- Acoustic analysis for robust speaker recognition-Distributed speaker recognition through UBM – GMM models –Hand Biometrics: Characterization by minutiae extraction –Sample Databases.

Unit V Multi biometrics and Visual Data Protection 9

Different principles of multi biometrics - Fusion levels - Applications and illustrations - Biometrics using ECG - Biometrics using medical imaging – Parametric and Non-parametric approaches for classification-Visual datahiding Security.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Enumerate the necessity of image processing
CO2	Enumerate various techniques for feature extraction
CO3	Analyze various techniques for object detection
CO4	Apply various tools for biometrics
CO5	Design data protection techniques

References

1. AmineNail-Ali and Regis Fournier "Signal and Image Processing for Biometrics" John Wiley and sons, 2012
2. Mark S.Nixon, Alberto S. Aguado, Feature Extraction and image processing for computer vision,ThirdEdition,,Elsevier2012.
3. Scott EBaugh "Digital Image Processing and analysis"2ndEdition CRCPress 2010

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22017 CYBER SECURITY MANAGEMENT AND CYBER LAWS **L T P C**
3 0 0 3

Course Objectives:

The students will be able to

1. Understand the need of Cyber Security
2. Explore the laws governing Cyber Security
3. Gain knowledge on Cyber Security Management

Unit I Fundamentals of Cyber Security 9

Introduction - Cyber Security and its problem - Intervention Strategies: Redundancy, Diversity and Autarchy.

Unit II Issues in CyberSecurity 9

Private ordering solutions, Regulation and Jurisdiction for global Cyber security, Copy Right-source of risks, Pirates, Internet Infringement, FairUse, postings, criminalliability, First Amendments, DataLoss.

Unit III Intellectual Property Rights 9

Copy Right-Source of risks, Pirates, Internet Infringement, Fair Use, postings, Criminal Liability,FirstAmendments,LosingData,Trademarks,Defamation,Privacy-Common Law Privacy, Constitutional law, Federal Statutes, Anonymity, Technology expanding privacy rights.

Unit IV Procedural Issues 9

Duty of Care, Criminal Liability, Procedural issues, Electronic Contracts & Digital Signatures, Misappropriation of information, CivilRights, Tax, Evidence.

Unit V Legal Aspects of CyberSecurity 9

Ethics, Legal Developments, Late1990 to 2000, Cyber security in Society, Security in cyberlaws case. studies, General law and Cyber Law -a Swift Analysis

TotalHours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Enumerate ethical laws of computer for different countries
CO2	Explore the needs on copyright issues of software
CO3	Analyze the issues those are specific to amendment rights
CO4	Demonstrate cyber security management skills
CO5	Explore the various options with IPR

References

1. JonathanRosenoer,“CyberLaw:ThelawoftheInternet”,Springer-Verlag,1997.
2. MarkFGrady,FransescoParisi,“TheLawandEconomicsofCyberSecurity”,CambridgeUniversityPress,2006
3. MichaelGraves,―DigitalArchaeology:TheArtandScienceofDigitalForensics,Addison-WesleyProfessional,2014

COURSE ARTICULATION MATRIX

COs	POs		
	1	2	3
1.	2	1	3
2.	3	1	3
3.	2	1	3
4.	2	1	3
5.	3	1	3

CF22008 NETWORK VIRTUALIZATION L T P C

3 0 0 3

Course Objectives:

The students will be able to

1. Understand the need for Virtualization
2. Get a practical knowledge on VMWare tools

Unit I Virtualization Fundamentals 9

Virtualization-need, Virtualization Technologies: Server Virtualization, Hardware emulation, Storage Virtualization, Network-attached storage, Storage area networks, I/O Virtualization, Network Virtualization, Client Virtualization, Application virtualization, Desktop virtualization,Case study: Studying Server Consolidation, Development and Test Environments , Quality of Service, Simple fail over High availability, Clustering, Data mirroring, Data replication, IT Operational Flexibility, Load balancing, Server pooling, Helping with Disaster Recovery, Rethinking Virtualizationin Business Terms: Rethinking Infrastructure Virtualization, Benefits ofV irtualization.

Unit II VMWare Virtualization 9

Virtual machines, and vSphere components, server, network, and storage virtualization, vSphere.Create Virtual Machine VMware vCenter Server: Introduction to vCenter Server architecture andappliance, Virtual Machine Management: Deploy virtual machines using templates and cloning,Modify and manage virtual machines, Create and manage virtual machine snapshots, Perform VMware vSphere vMotion and Storage vMotion migrations, Create a vSpherev App.

UnitIII Access and Authentication Control 9

Control user access through roles and permissions, Configure and manage the ESXi firewall, Configure ESXi lock down mode, Integrate ESXi with Active Directory, Introduce VMware vShield Zones.

UnitIV Installing VMWare Components 9

Introduce ESXi installation, Describe boot from SAN requirements, Introduce vCenter Serverdeployment options, Describe vCenter Server hardware, software, and database requirements, Install vCenter Server(Windowsbased).

UnitV Implement and Configure WindowServer2008 HyperV 9

Configure Hyper V Virtual Networking, Configure and use HyperV remote administration, Create and configure Virtual Hard Drives, Use Virtual Machine snapshots, Describe considerations for configuring Hyper-V servers for high availability, Virtual Machine Manager(VMM)features and use VMM to manage virtual machines.

Total Hours:45

CourseOutcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Enumerate the features of network virtualization
CO2	Demonstrate VMWare tools
CO3	Configure the system using Virtualization tools
CO4	Analyse the various requirements for VMware
CO5	Experiment various roles in Access and authentication control

References

1. Virtualization:a beginner's guide-DanielleRuest,NelsonRuest,McGraw-Hill ProfMed, 2010.
2. Windows Server 2008 Hyper-V: Insiders Guide to Microsoft's Hypervisor By JohnKelbley, MikeSterling,AllenStewart,Sybex;1edition(April20,2009).
3. VirtualizationforDummies-BernardGolden,ForDummies;1edition(December5,2007).
4. Mastering Microsoft Virtualization-TimCerling, JeffreyBuller, JeffreyL.Buller, Sybex;1edition(December21,2009).

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22010 CLOUD COMPUTING TECHNOLOGIES L T P C

3 0 0 3

Course Objectives:

The students will be able to

1. Gain knowledge on the concept of virtualization that is fundamental to cloud computing
2. Understand the various issues in cloud computing
3. Be able to setup a private cloud

Unit I Virtualization In Cloud 9

Basics of Virtual Machines-Process Virtual Machines–System Virtual Machines–Emulation –Interpretation–Binary Translation-Taxonomy of Virtual Machines. Virtualization–Management Virtualization—Hardware Maximization–Architectures–Virtualization Management–Storage Virtualization–Network Virtualization.

Unit II Virtualization Infrastructure 9

Comprehensive Analysis – Resource Pool–Testing Environment–Server Virtualization–Virtual Workloads – Provision Virtual Machines – Desktop Virtualization–Application Virtualization - Implementation levels of virtualization– virtualization structure – virtualization of CPU, Memory and I/O devices–virtual clusters and Resource Management – Virtualization for data center automation.

Unit III Cloud Platform Architecture 9

Cloud deployment models: public, private, hybrid, community – Categories of cloud computing: Everything as a service: Infrastructure, platform, software -A Generic Cloud Architecture Design– Layered cloud Architectural Development – Virtualization Support and Disaster Recovery –Architectural Design Challenges - Public Cloud Platforms : GAE,AWS – Inter-cloud ResourceManagement.

Unit IV Programming Model 9

Introduction to Hadoop Framework- Mapreduce,Input splitting,map and reduce functions, specifying input and output parameters, configuring and running a job –Developing Map Reduce Applications - Design of Hadoop file system–Setting up Hadoop Cluster - Cloud Software Environments-Eucalyptus, OpenNebula, OpenStack, Nimbus.

Unit V Cloud Security 9

Cloud Infrastructure security: network, host and application level – aspects ofdata security, provider data and its security, Identity and access management architecture, IAM practices in thecloud, SaaS, PaaS, IaaS availability in the cloud - Key privacy issues in the cloud –Cloud Security and Trust Management.

TotalHours:45

CourseOutcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Examine the concepts of virtualization and virtual machines
CO2	Integrate the knowledge on the concept of virtualization that is fundamental to cloud computing
CO3	Interpret various security issues in Cloud Computing
CO4	Develop a private cloud for different applications
CO5	Inspect the security issues in the grid and the cloud environment

References

1. DanielleRuest,NelsonRuest,"Virtualization:ABeginner‟sGuide",McGraw-HillOsborneMedia,2009.
2. JimSmith,RaviNair,"VirtualMachines:VersatilePlatformsforSystemsandProcesses",Elsevier/MorganKaufmann,2005
3. JohnW.RittinghouseandJamesF.Ransome,"CloudComputing:Implementation,Management,andSecurity",CRCPress,2010.
4. KaiHwang,GeoffreyCFox,JackGDongarra,"DistributedandCloudComputing,FromParallelProcessingtotheInternetofThings",MorganKaufmannPublishers,2012.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

		L	T	P	C
CF22001	**ENERGY AWARE COMPUTING**	**L**	**T**	**P**	**C**
		3	**0**	**0**	**3**

Course Objectives:

The students will be able to

1. Understand the fundamentals of Energy Efficient Computing
2. Understand the concept of Energy Efficient Storage Systems
3. Introduce the various types of scheduling algorithms in energy-efficient computing
4. Introduce the concept of Green Networking
5. Study Energy Aware Applications

Unit I Introduction 9

Subreshold Computing –Energy Efficient Network-on-Chip Architectures for Multi-CoreSystems-Energy-Efficient MIPS CPU Core with Fine-Grained Run-Time Power Gating –LowPower design of Emerging memory technologies.

Unit II Energy Efficient Storage 9

Disk Energy Management- Power Efficient Strategies for Storage Systems-Dynamic thermal management for high performance storage systems- Energy-Saving Techniques for Disk StorageSystems.

Unit III Energy Efficient Scheduling Algorithms 9

Algorithms and Analysis of Energy-Efficient Scheduling of Parallel Tasks- Dynamic Voltage Scaling-Speed Scaling-Processor optimization- Online job scheduling Algorithms.

Unit IV Green Networking 9

Power-Aware Middleware for Mobile Applications - Energy Efficiency of Voice-over-IPSystems - Intelligent Energy - Aware Networks - Green T CAM-Based Internet Routers.

Unit V Energy Aware Computing Applications 9

On-Chip Network - Video Codec Design - Energy Aware Surveillance Camera -Low Power Design Challenge in Biomedical Implant Electronics.

TotalHours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Design Power efficient architecture Hardware and Software
CO2	Analyze the different types of Energy Efficient Storage systems.
CO3	Design the algorithms for Energy Efficient Systems
CO4	Identify the different types of Green Networking schemes in the energy efficient computing
CO5	Explore the applications of Energy Aware Computing

References

1. Bobsteigerwald,Chris:Luero,EnergyAwarecomputing,IntelPress,2012
2. Chong-MinKyung,Sungiooyoo,EnergyAwaresystemdesignAlgorithmsandArchitecture,Springer,2011.
3. IshfaqAhmad,SanjayRanka,HandbookofEnergyAwareandGreenComputing,CRCPress,2012

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22003 ADVANCED INFRASTRUCTURE MANAGEMENT L T P C
3 0 0 3

Course Objectives:

The students will be able to

1. Understand the requirements of Infrastructure management
2. Get a firm knowledge on various storage technologies
3. Know the need for network and cloud management

Unit I Infrastructure Management Overview 9

Infrastructure management activities, Preparing for Infrastructure Management Factors to consider in designing IT organizations and IT infrastructure, Determining customer's Requirements, Identifying System Components to manage, Exist Processes, Data, applications,Tools and their integration, Patterns for IT systems management, Introduction to the design process for information systems, Models, Information Technology Infrastructure Library(ITIL).

Unit II Different Storage Technologies and Virtualization 9

Challenges in Data Storage and Management, Data Storage Infrastructure. Components of a Storage System Environment, Intelligent Storage System (ISS) and its components, Introduction to Networked Storage: Evolution of networked storage, Architecture, Overview of FC-SAN, NAS, and IPSAN. Network-Attached Storage(NAS): BenefitsofNAS,Components,Implementations,FileSharing,I/Ooperations,ContentAddressedStorage(CAS):CASArchitecture,StorageandRetrieval,Examples.StorageVirtualization: Forms,Taxonomy,Configuration,Challenges,TypesofStorageVirtualizations.

Unit III Network Infrastructure 9

Implementing, Managing and Maintaining IP Addressing; Configure TCP/IP addressing on aserver computer using DHCP; Implementing, Managing and Maintaining Name Resolution usingDNS Server; Implementing, Managing and Maintaining Routing and Remote Access; Configure remote access authentication protocols; Implement secure access between private networks; Manage Routing and Remote Access routing interfaces; Maintaining a Network Infrastructure.

Unit IV Cloud Infrastructure 9

Architectural Design of Compute and Storage Clouds, Layered Cloud Architecture Development, Design Challenges, Inter Cloud Resource Management, Resource Provisioning and Platform Deployment, Global Exchange of Cloud Resources. Administrating the Clouds, Cloud Management Products, Emerging Cloud Management Standards.

Unit V CaseStudy 9

Devops Infrastructure Management, Container Infrastructure Management, Engine yard PaaS, Docker Infrastructure Management.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Examine the Infrastructure management activities
CO2	Explore the different storage technologies
CO3	Manage and Maintain Routing and Remote Access
CO4	Develop Layered Cloud Architecture
CO5	Explore Devops, Container and Docker Infrastructure Management

References

1. G.Somasundaram, AlokShrivastava, EMCEducationalServices, Information Storage and Management,WileyIndia.
2. RobertSpalding,“StorageNetworks:TheCompleteReference“,TataMcGrawHill,Osborne,2003.
3. MarcFarley,“BuildingStorageNetworks”,TataMcGrawHill,Osborne,2001.
4. JanVanBon,“FoundationsofITServiceManagement:basedonITIL”,VanHarenPublishing,2005.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22019 MALWARE ANALYSIS AND REVERSE ENGINEERING

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

1. Gain in-depth knowledge on fundamentals of malware analysis.
2. Use JIT compilers formal ware detection in legitimate code.
3. Implement DNS filtering and apply reverse engineering.

Unit I Introduction to Malware Analysis 9

Introduction to key MA tools and techniques,Understanding Malware Threats, Malware indicators, Malware Classification, Introduction to MASandboxes Capturing and Analyzing Network Traffic, Internet simulation using INetSim, Using Deep Freeze to Preserve Physical Systems, Using FOG for Cloning and Imaging Disks.

Unit II Reverse Engineering Malware 9

Behavioural Analysis vs. Code Analysis, Resources for Reverse-Engineering Malware (REM) -Examining Clam AV Signatures, Creating Custom Clam AV Databases, Using YARA to Detect Malware Capabilities.

Unit III Malware Forensics 9

UsingTSKforNetworkandHostDiscoveries,UsingMicrosoftOfflineAPItoRegistryDiscoveries ,Identifying Packers using PEiD, Registry Forensics with RegRipper Plugins:, Bypassing Poison Ivy’s Locked Files, Bypassing Conficker’s File System ACL Restrictions, Detecting Rogue PKI Certificates.

Unit IV Malware and Kernel Debugging 9

Opening and Attaching to Processes, Configuration of JIT Debugger for Shellcode Analysis,ControllingProgramExecution,SettingandCatchingBreakpoints,DebuggingwithPythonScripts and Py Commands, DLL Export Enumeration, Execution, and Debugging, Debugging a VMware Workstation Guest(onWindows), Debugging a Parallels Guest(onMacOSX).

Unit V Memory Forensics and Volatility 9

Memory Dumping with MoonSols Windows Memory Toolkit, Accessing VM Memory FilesOverviewofVolatility,InvestigatingProcessesinMemoryDumps,CodeInjectionandExtraction,DetectingandCapturingSuspiciousLoadedDLLs,FindingArtifactsinProcessMemory,IdentifyingInjectedCodewithMalfindandYARA.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Apply the concept of malware and reverse engineering.
CO2	Implement tools and techniques of malware analysis.
CO3	Perform Malware and kernel debugging
CO4	Perform forensics on memory
CO5	Experiment with proactive and defensive measures to deter and repel potential threats

References

1. MichaelSikorski, AndrewHonig, Practical Malware Analysis: TheHands -On Guide to Dissecting Malicious Software publisherWilliamPollock,2012.
2. MichaelHaleLigh,AndrewCase,JamieLevy,AAronWalters,The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and MacMemory,1st Edition, 2014.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22021 DATA ANALYTICS AND BUSINESS INTELLIGENCE

L	T	P	C
3	0	0	3

Course Objectives:

The students will be able to

1. Understand linear and logistic regression models
2. Understand simulation using regression models
3. Understand data collection and model understanding

Unit I Linear Regression 9

Introduction to data analysis – Statistical processes – statistical models – statistical inference –review of random variables and probability distributions – linear regression – one predictor –multiplepredictors–predictionandvalidation–lineartransformations–centeringandstandardizing– correlation– logarithmic transformations– other transformations –building regression models– fitting a series of regressions.

Unit II Logistic and Generalized Linear Models 9

Logistic regression – logistic regression coefficients – latent - dataformulation –building a logistic regression model – logistic regression with interactions – evaluating, checking, and comparing fitted logistic regressions – identifiability and separation–Poisson regression – logistic-binomial model – Probit regression – multinomial regression – robust regression using tmodel–building complex generalized linear models–constructive choice models.

Unit III Simulation and Causal Inference 9

Simulation of probability models – summarizing linear regressions – simulation of non-linear predictions–predictive simulation for generalized linear models–fake-data simulation–simulating and comparing to actual data – predictive simulation to check the fit of a time-seriesmodel – causal inference – randomized experiments – observational studies – causal inference using advanced models– matching–instrumental variables.

Unit IV Multilevel Regression 9

Multilevel structures – clustered data – multilevel linear models – partial pooling – group-level predictors – model building and statistical significance – varying intercepts and slopes – scaled inverse-Wishart distribution – non-nested models – multi-level logistic regression – multi-level generalized linear models.

Unit V Data Collection and Model Understanding 9

Design of data collection – classical power calculations – multilevel power calculations – power calculation using fake - data simulation–understanding and summarizing fitted models–uncertainty and variability – variances – R2 and explained variance – multiple comparisons and statistical significance – analysis of variance – ANOVA and multilevel linear and general linear models–missing data imputation.

Total Hours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Demonstrate logistic and Generalized Linear Models
CO2	Develop simulation using regression models
CO3	Perform casual inference from data
CO4	Build multilevel regression models
CO5	Inspect data collection and variance analysis

References

1. Andrew Gelman and Jennifer Hill, "Data Analysis using Regression andmultilevel/HierarchicalModels",CambridgeUniversityPress,2006.
2. PhilippK.Janert,"DataAnalysiswithOpenSourceTools",O'Reilley,2010.
3. DavinderjitSiviaandJohnSkilling,"DataAnalysis:ABayesianTutorial,SecondEdition,OxfordUniversityPress,2006.
4. Robert Nisbelt, JohnElder, andGaryMiner, "Handbook of statistical analysis and datamining applications",AcademicPress,2009.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**

CF22023 WIRELESS SECURITY L T P C

3 0 0 3

Course Objectives:

The students will be able to

1. Gain in- depth knowledge on wireless and mobile network security and it relation to the new security based protocols.
2. Apply proactive and defensive measures to counter potential threats, attacks and intrusions.
3. Design secured wireless and mobile networks that optimise accessibility whilst minimising vulnerability to security risks.

Unit I Introduction 9

Uniqueness of wireless - Wireless Information Warfare -Taxonomies of Wireless Communication Networks - Information Theory - Decision Theory - A Model for cost effective risk management - Performance measures.

Unit II Security inWLAN 9

Wireless Transmission Media, WLAN Products and standards securing WLAN-counter measures - WAP - WTLS - Bluetooth - VoIP.

Unit III Security in cellular Networks 9

Threats, Hacking and Viruses in mobile communications- Access control and Authentication in mobile communications.

Unit IV Security in Adhoc Networks 9

Adhoc Networking - Major Routing Protocol in Adhoc Networks -Attack against AdHoc Networks, Securing Adhoc Networks - Authentication in Adhoc Networks–key Management– Intrusion Detection in Adhoc Networks

Unit V Security in RFID 9

Multitag RFID systems - Attacking RFID systems - RFID Relayattacks-Physical privacy and security in RFID systems- Authentication Protocol in RFID systems-Lightweight Cryptography for Low-Cost RFID tags.

TotalHours:45

Course Outcomes:

At the end of the course, the students will be able to,

CO	*CO statements*
CO1	Enumerate advanced security and privacy issues in wireless systems, including cellular and wirelessLAN
CO2	Analyze state-of-the-art technologies and protocols of wireless network security
CO3	Identify and investigate in-depth both early and contemporary threats to mobile and wireless networks security
CO4	Analyze the various aspects of security in RFID
CO5	Apply proactive and defensive measures to deter and repel potential threats, attacks and intrusions

References

1. Nichols,RandallK.;Lekkas,Panos,"WirelessSecurity:Models,Threats,AndSolutions", McGraw HillProfessional,2002.
2. YanZhangandParisKitsos,"SecurityinRFIDandSensorNetworks",CRCPRESS,2009.
3. NoureddineBoudriga,"SecurityofMobileCommunications",ISBN9780849379413,2010.

COURSE ARTICULATION MATRIX

COs	**POs**		
	1	**2**	**3**
1.	**2**	**1**	**3**
2.	**3**	**1**	**3**
3.	**2**	**1**	**3**
4.	**2**	**1**	**3**
5.	**3**	**1**	**3**